

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-077473

(43)Date of publication of application : 15.03.2002

(51)Int.Cl.

H04N 1/00

G06F 13/00

(21)Application number : 2000-254883

(71)Applicant : MURATA MACH LTD

(22)Date of filing : 25.08.2000

(72)Inventor : TANIMOTO YOSHIFUMI

## (54) NETWORK SCANNER

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a network scanner capable of ensuring security for distribution of image data to a distribution destination terminal device.

**SOLUTION:** When a user of a communication terminal device connected to a communication network, such as LAN, accesses a folder storing image data formed by the network scanner, an attribute of security for the image data is determined for each user to ensure security of the image data to be distributed. The attribute of the security is determined, based on a table in which items capable of being dealt with by each user are made to correspond to the image data. For example, image data of a user's name 'yamamoto' can be subjected to processes, such as reading and editing, but it cannot be subjected to processes such as erasure and printing.

ユーザ名	閲覧	編集	削除	印刷
YAMAMOTO	○	○	×	×
TANIMOTO	○	○	○	○
SMITH	○	×	×	×
JOHNSON	○	×	○	×

## LEGAL STATUS

[Date of request for examination] 18.12.2001

[Date of sending the examiner's decision of rejection] 14.10.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

**\* NOTICES \***

**JPO and NCIPi are not responsible for any damages caused by the use of this translation.**

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

**CLAIMS**

---

[Claim(s)]

[Claim 1] The network scanner characterized by to store and store the drawing data with which the attribute of said security was given to the folder which was connected to the communication network with equipment in the end of a distribution tip, is the network scanner which forms the drawing data of a reading image and is distributed to equipment in the end of a distribution tip, was equipped with a means to give the attribute of security for said every drawing data, and was set as the communication network.

[Claim 2] The network scanner according to claim 1 characterized by setting said folder as either of equipment, or its both in a network scanner and the end of a distribution tip.

[Claim 3] Said attribute is a network scanner according to claim 1 or 2 characterized by setting up the item over each drawing data which can be processed for every user.

---

[Translation done.]

**\* NOTICES \***

**JPO and NCIPi are not responsible for any damages caused by the use of this translation.**

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

**DETAILED DESCRIPTION**

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the network scanner which can secure the security at the time of distributing drawing data to equipment in the end of a distribution tip.

[0002]

[Description of the Prior Art] The application of an image reader (scanner) is being expanded with progress of the latest communication technology and computer technology. The network scanner which distributes to equipment the drawing data which connected equipment with the scanner in the end of a distribution tip, and were formed in a communication network like a user local area network (it is written as LAN LocalArea Network and the following.) with the scanner as the example in said end of a distribution tip is known.

[0003] A communication terminal like a fax server (in this specification and a drawing, it is hereafter written as a FAX server.) as a scanner which distributes said drawing data is used. In this case, the FAX server concerned acts as a network scanner. Moreover, as equipment, communication terminals, such as a file server and a KURAIANTOPA-SONARU computer (it is hereafter written as Client PC.), are connected to the communication network in the end of a distribution tip.

[0004] A manuscript is read with a network scanner and the formed drawing data are stored in the folder of the communication terminal connected to communication networks, such as a network scanner or a file server. In this case, the file of drawing data is accumulated in the folder concerned one by one by giving a file name to each drawing data.

[0005]

[Problem(s) to be Solved by the Invention] Thus, sequential are recording of the drawing data with which it was formed with the network scanner and the file name was given is carried out at a predetermined folder. This folder is shared by each communication terminal connected to the communication network, and a user can access said folder from any communication terminal. For this reason, there was a problem that security for every drawing data was not securable.

[0006] This invention aims at offer of the network scanner which can secure the security at the time of distributing drawing data to equipment in the end of a distribution tip in view of the above problems.

[0007]

[Means for Solving the Problem] In invention which the above-mentioned purpose of this invention requires for claim 1 a network scanner It is the network scanner which is connected to a communication network with equipment in the end of a distribution tip, forms the drawing data of a reading image, and is distributed to equipment in the end of a distribution tip. It has a means to give the attribute of security for said every drawing data, and is attained by considering as the configuration which stores and stores the drawing data with which the attribute of said security was given to the folder set as the communication network.

[0008] Moreover, invention concerning claim 2 is characterized by setting said folder as either of equipment, or its both in a network scanner and the end of a distribution tip in the network scanner according to claim 1.

[0009] Moreover, in the network scanner according to claim 1 or 2, said attribute is characterized by setting up the item over each drawing data which can be processed for every user by invention concerning claim 3.

[0010] According to the description of invention concerning above-mentioned claim 1, the attribute of security is given to the drawing data which are stored in a folder and distributed to equipment in the end of a distribution tip. For this reason, the security for every drawing data is securable.

[0011] Moreover, in invention concerning claim 2, the folder which stores and stores the drawing data with which the attribute of security was given is set as either of equipment in a network scanner and the end of a

distribution tip. Thus, if a folder is set as a certain communication terminal connected to the communication network, in other communication terminals, it is not necessary to set up a folder, and is considering as the configuration which can share a folder between the communication terminals connected to the communication network, and a memory resource can be saved.

[0012] Moreover, a case when a folder was assigned to both of equipment in a network scanner and the end of a distribution tip, as for example, the network scanner was moved to other networks, and even when the folder of a network scanner is damaged, the reconstitution of data can be performed easily.

[0013] Furthermore, in invention concerning claim 3, as for the attribute of security, the item over each drawing data which can be processed is set up for every user. For this reason, for every drawing data, it becomes clear what kind of processing can be performed, and a specific user can raise the security at the time of distributing drawing data.

[0014]

[Embodiment of the Invention] Hereafter, drawing explains the gestalt of operation of the network scanner concerning this invention. Drawing 3 is the block diagram of an outline showing one gestalt of the communication network where the network scanner of this invention is used. In drawing 3 R> 3, the FAX server 1 which acts as a network scanner, the file server 2 which is equipment in the distribution tip end of drawing data, the client PC 3, and the printer 4 are connected to LAN5.

[0015] It shall read by the FAX server 1, the drawing data of an image shall be formed, and said drawing data shall be distributed to equipment in the end of a distribution tip it connects with LAN5. If a file server 2 is a distribution place, the drawing data outputted from the FAX server 1 will be inputted into the folder set as the file server 2 in the path of Da through LAN5.

[0016] Moreover, drawing data are inputted into the folder set as each communication terminal through LAN5 also when a client PC 3 and a printer 4 are distribution places. In addition, it can also consider as the configuration which shares the folder set as said file server 2 between each communication terminal connected to LAN5. In this case, the drawing data with which the file name was given and distributed from the network scanner are stored and stored in the folder set as the file server 2 one by one.

[0017] Thus, processing of each communication terminal in the case of considering as the configuration which shares the folder set as the file server 2 on a communication network is explained. A client PC 3 accesses said folder of a file server 2 in the path of Db through LAN5, and processes perusal of drawing data etc. Similarly, a printer 4 accesses said folder of a file server 2 in the path of Dc through LAN5, and processes printing of drawing data etc.

[0018] In this invention, in case the user of the communication terminal connected to communication networks, such as LAN, accesses the folder in which the drawing data formed with the network scanner are stored, for every user, the attribute of the security to the drawing data concerned is set up, and is considered as the configuration which can secure the security to the drawing data distributed.

[0019] Drawing 2 is the explanatory view showing the example of the data configuration stored in a folder. In drawing 2, the part of (b) is drawing data which read the manuscript and were formed with the network scanner. The part of (a) is the attribute (the item of the processing authority which can carry out processing to drawing data to which level, or is permitted by the user is shown) of the security given to drawing data (b), and is set up for every drawing data.

[0020] Drawing 1 is the explanatory view showing the example of said attribute. The attribute of security makes a user name and the item which can be processed correspond to drawing 1 on a table so that it may be shown. As an item which can be processed, "perusal" about the drawing data concerned, "edit", "elimination", and "printing" are illustrated.

[0021] In said each item, O mark is given to the item which has processing authority to a user, and x mark is given to the item without processing authority. For example, a user name "yamamoto" cannot perform processing of elimination and printing, although perusal of the drawing data concerned and processing of edit are possible. Moreover, a user name "satoh" cannot perform processing of edit, elimination, and printing, although processing of perusal of the drawing data concerned is possible.

[0022] On the table of the attribute of security shown in drawing 1, although the user name is written with the alphabet, it can also write by each user's identifier (ID). In addition, when the drawing data concerned are formed by two or more pages, the user who can do processing of "perusal", "edit", "elimination", and "printing" for every page may be set up according to an individual.

[0023] The attribute of security shown in drawing 1 can be beforehand set up as an item of the processing authority of a user proper. For example, to all drawing data, only processing of perusal is possible for the above "satoh", and it sets up processing of other items with an improper thing. Moreover, the item of the

processing authority permitted by the user is changeable for every drawing data.

[0024] For example, although processing of perusal of a certain drawing data is possible, said user "sato" sets up processing of perusal of other drawing data as it is improper. The attribute of security as shown in drawing 1 is set up by control units, such as an input key, a mouse, etc. which were installed in the network scanner. The shared folder which gave the attribute of such security is set as the FAX server 1, and also it can be set to other communication terminals connected to the communication network as mentioned above, for example, a file server.

[0025] If a shared folder is set as the FAX server 1, since other communication terminals connected to the communication network can use the shared folder set as said FAX server 1, a memory resource can be saved. Moreover, if a shared folder is set as a communication terminal besides the above, the memory resource of the FAX server 1 can be saved.

[0026] Furthermore, the shared folder set as the FAX server 1 can be copied, and the same shared folder as other communication terminals can also be set up. in this case -- for example, a case as the FAX server 1 was moved to other networks, and even when the shared folder of the FAX server 1 is damaged, the reconstitution of data can be performed easily.

[0027] Drawing 4 is the block diagram of an outline showing an example of the control device 20 formed in the FAX server applied to this invention. In drawing 4, a micro processing unit (it is hereafter written as MPU) for 21 to process various signals and data, the data which need 22 for various actuation of a FAX server and ROM by which program storing is carried out, and 23 are RAM in which management data etc. is stored.

[0028] The read station which the printer by which 24 outputs drawing data to the detail paper, and 25 read a manuscript, and outputs the drawing data which are a monochrome binary image data, and 26 are control units which consist of a keyboard, a mouse, etc. A FAX server is connected to LAN5 through a network interface (I/F) 27. A FAX server is connected to ISDN through the interface (I/F) 28 of an integrated services digital network (ISDN), and a digital service unit (DSU) 29. Moreover, it connects with a public line network (PSTN) through the line control section (NCU) 30.

[0029] 31 is a modem which modulates . restores to FAKUSHIMIRIDE-TA transmitted and received between a phase hand's facsimile apparatus through PSTN, and a modem 31 and NCU30 are connected by analog signal line 31a.

[0030] A sign and the decode section 32 encode drawing data, and decrypts drawing data. The graphic-character generating section 33 changes character code data into an image data. The clock section used in order that the display for which 34 used the cathode-ray tube (CRT) and the liquid crystal display (LCD), and 35 may write down time in drawing data, the hard disk (HD) with which 36 memorizes communication management record and drawing data, and 37 are internal buses. In addition, when you do not need memory capacity so much, it replaces with a hard disk (HD) and uses an image memory.

[0031] Drawing 5 is a flow chart which shows the procedure of the network scanner of this invention. Next, this flow chart is explained.

[0032] (1) Start the processing program of a network scanner at step S1, and set a reading manuscript by processing of step S2. Next, it shifts to processing of step S3, and the destination of the shared folder which stores drawing data, and the attribute of security are specified.

[0033] (2) Next, read a manuscript by processing of step S4 and perform coding processing of drawing data. Then, an attribute and drawing data are stored in an image memory by processing of step S5, and a processing program is ended at step S6.

[0034] Drawing 6 is a flow chart which shows the procedure of the client PC which accesses drawing data. Next, this flow chart is explained.

[0035] (1) Start the processing program of Client PC at step S11, and perform file designation accessed by processing of step S12. Next, a security attribute is checked by processing of step S13. Then, it judges whether it has the authority which a user accesses by processing of step S14 to the file of the folder in which drawing data were stored. If this judgment result is NO, a processing program will be ended at step S16.

[0036] (2) If the judgment result of step S14 is YES, since the user will have the authority to access a file, shift to processing of step S15. In processing of step S15, processing permitted in processings, such as perusal, edit, elimination, and printing, about the drawing data of the file name concerned is performed. Next, a processing program is ended at step S16.

[0037] In drawing 3, other FAX servers can be connected to LAN5, and drawing data can also be distributed to other FAX servers from the FAX server 1. in this case -- being concerned -- others -- a FAX server acts as equipment in the distribution tip end of the FAX server 1.

[0038] moreover -- being concerned -- others -- a FAX server can read drawing data from the shared folder set as the file server 2, and can distribute to other communication terminals. furthermore -- being concerned -- others -- the attribute of security can be given to the drawing data which read the manuscript and were formed by the FAX server, and it can store in the folder of the self-inside of a plane set up as a shared folder.

[0039]

[Effect of the Invention] According to invention which relates to claim 1 as explained in full detail above, the attribute of security is given to the drawing data which are stored in a folder and distributed to equipment in the end of a distribution tip. For this reason, the security for every drawing data is securable.

[0040] Moreover, in invention concerning claim 2, the folder which stores and stores the drawing data with which the attribute of security was given is set as either of equipment in a network scanner and the end of a distribution tip. Thus, if a folder is set as a certain communication terminal connected to the communication network, in other communication terminals, it is not necessary to set up a folder, and is considering as the configuration which can share a folder between the communication terminals connected to the communication network, and a memory resource can be saved.

[0041] Moreover, a case when a folder was assigned to both of equipment in a network scanner and the end of a distribution tip, as for example, the network scanner was moved to other networks, and even when the folder of a network scanner is damaged, the reconstitution of data can be performed easily.

[0042] Furthermore, in invention concerning claim 3, as for the attribute of security, the item over each drawing data which can be processed is set up for every user. For this reason, for every drawing data, it becomes clear what kind of processing can be performed, and a specific user can raise the security at the time of distributing drawing data.

---

[Translation done.]

## \* NOTICES \*

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

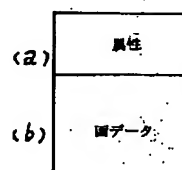
1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

## DRAWINGS

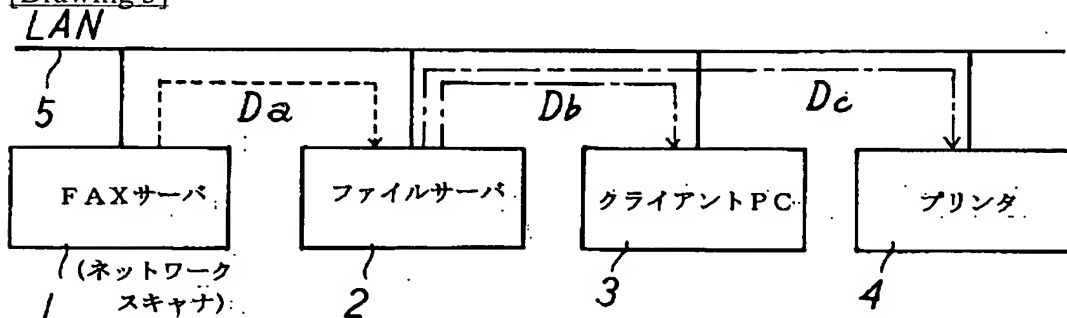
[Drawing 1]

ユーザ	項目	閲覧	編集	削除	印刷
yanamoto		○	○	×	×
tanaka		○	○	○	○
sato		○	×	×	×
data		○	×	○	×

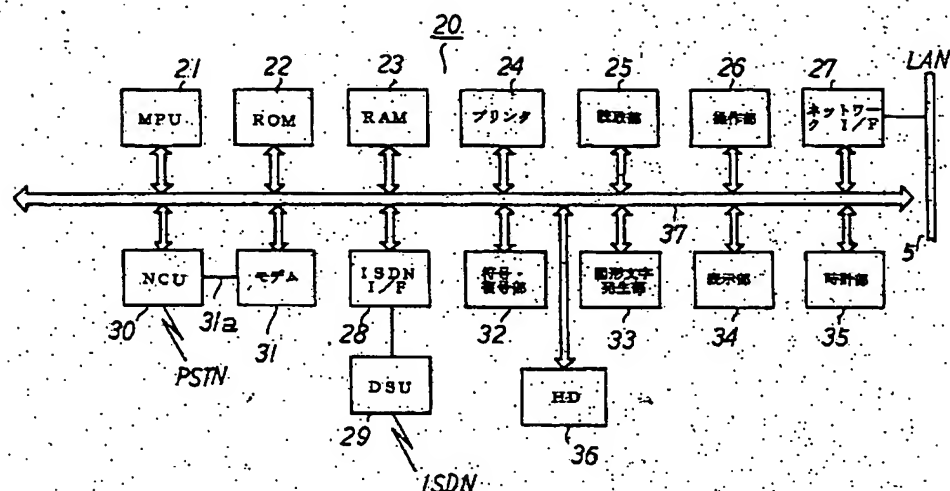
[Drawing 2]



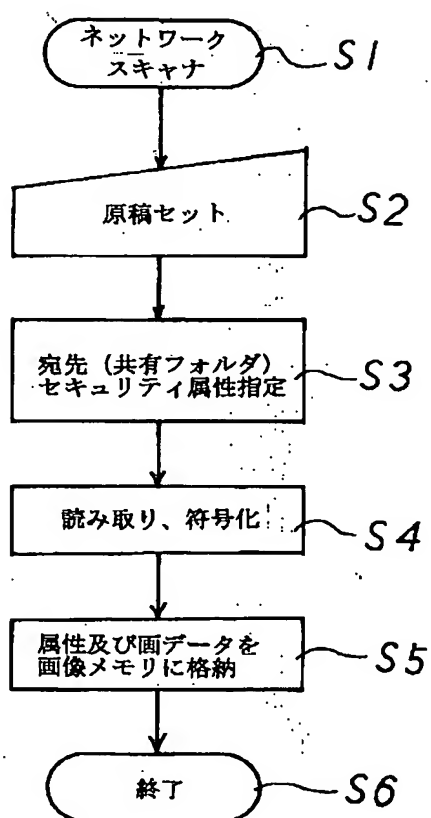
[Drawing 3]



[Drawing 4]

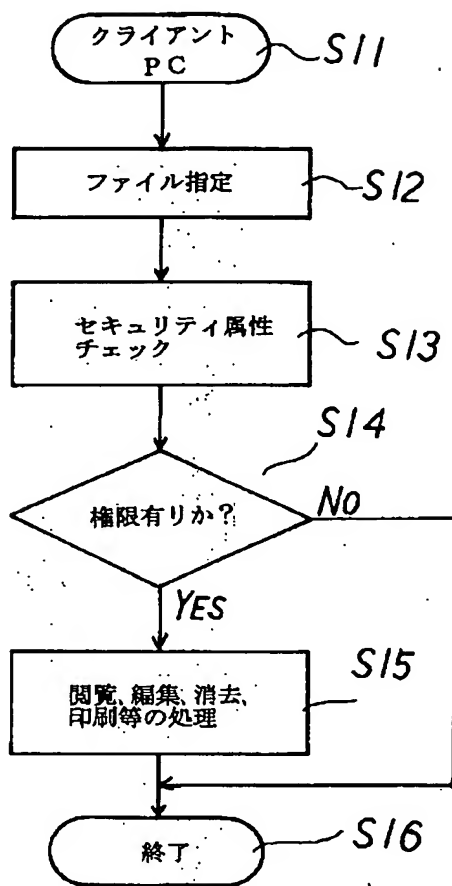


[Drawing 5]



[Drawing 6]





[Translation done.]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-77473  
(P 2002-77473A)  
(43) 公開日 平成14年3月15日 (2002.3.15)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テマコード (参考)
H04N 1/00		H04N 1/00	C 5C062
G06F 13/00	640	G06F 13/00	640

審査請求 未請求 請求項の数 3 O L (全7頁)

(21) 出願番号	特願2000-254883 (P 2000-254883)	(71) 出願人	000006297 村田機械株式会社 京都府京都市南区吉祥院南落合町3番地
(22) 出願日	平成12年8月25日 (2000.8.25)	(72) 発明者	谷本 好史 京都市伏見区竹田向代町136番地 村田機械株式会社本社工場内
		(74) 代理人	100103791 弁理士 川崎 勝弘 (外1名)
		Fターム (参考)	5C062 AA05 AA13 AA30 AA35 AB17 AB42 AC02 AC22 AF12

(54) 【発明の名称】 ネットワークスキャナ

(57) 【要約】

【課題】 配信先端末装置に画データを配信する際のセキュリティが確保できるネットワークスキャナを提供すること。

【解決手段】 LAN等の通信ネットワークに接続された通信端末装置のユーザが、ネットワークスキャナで形成された画データが格納されているフォルダにアクセスする際に、ユーザ毎に当該画データに対するセキュリティの属性を設定して、配信される画データに対するセキュリティが確保できる構成とする。セキュリティの属性は、各ユーザが前記画データに対して処理可能な項目を対応させたテーブルで設定する。例えばユーザ名「yamamoto」は、当該画データの閲覧、編集の処理は可能であるが、消去、印刷の処理はできない。

ユーザ \ 項目	閲覧	編集	消去	印刷
yamamoto	○	○	×	×
tanaka	○	○	○	○
isioh	○	×	×	×
inoue	○	×	○	×

## 【特許請求の範囲】

【請求項 1】 通信ネットワークに配信先端末装置と共に接続され、読み取り画像の画データを形成して配信先端末装置に配信するネットワークスキャナであって、前記画データ毎にセキュリティの属性を付与する手段を備え、通信ネットワークに設定されたフォルダに前記セキュリティの属性が付与された画データを格納して蓄積することを特徴とするネットワークスキャナ。

【請求項 2】 前記フォルダをネットワークスキャナと配信先端末装置のいずれか、またはその両者に設定することを特徴とする、請求項 1 に記載のネットワークスキャナ。

【請求項 3】 前記属性は、ユーザ毎に各画データに対する処理可能な項目が設定されることを特徴とする、請求項 1 または請求項 2 に記載のネットワークスキャナ。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、配信先端末装置に画データを配信する際のセキュリティが確保できるネットワークスキャナに関するものである。

## 【0002】

【従来の技術】 最近の通信技術やコンピュータ技術の進展に伴い、画像読取装置（スキャナ）の用途が拡大してきている。その一例として、ユーザ構内通信網（Local Area Network、以下、LAN と略記する。）のような通信ネットワークに、スキャナと配信先端末装置とを接続し、スキャナで形成された画データを前記配信先端末装置に配信するネットワークスキャナが知られている。

【0003】 前記画データを配信するスキャナとして、例えばファクスサーバ（以下、本明細書および図面では FAX サーバと略記する。）のような通信端末装置が使用される。この場合には、当該 FAX サーバはネットワークスキャナとして作用する。また、配信先端末装置としては、ファイルサーバやクライアントパーソナルコンピュータ（以下、クライアント PC と略記する。）等の通信端末装置が通信ネットワークに接続されている。

【0004】 ネットワークスキャナで原稿を読み取り、形成された画データは、ネットワークスキャナまたはファイルサーバ等の通信ネットワークに接続された通信端末装置のフォルダに格納される。この際に、各画データにファイル名を付与することにより、当該フォルダには、順次画データのファイルが蓄積される。

## 【0005】

【発明が解決しようとする課題】 このように、ネットワークスキャナで形成されてファイル名が付与された画データは、所定のフォルダに順次蓄積される。このフォルダは、通信ネットワークに接続された各通信端末装置で共有されており、いずれの通信端末装置からもユーザは前記フォルダにアクセスできる。このため、画データ毎

のセキュリティを確保することができないという問題があった。

【0006】 本発明は上記のような問題に鑑み、配信先端末装置に画データを配信する際のセキュリティが確保できるネットワークスキャナの提供を目的とする。

## 【0007】

【課題を解決するための手段】 本発明の上記目的は、請求項 1 に係る発明において、ネットワークスキャナを、通信ネットワークに配信先端末装置と共に接続され、読み取り画像の画データを形成して配信先端末装置に配信するネットワークスキャナであって、前記画データ毎にセキュリティの属性を付与する手段を備え、通信ネットワークに設定されたフォルダに前記セキュリティの属性が付与された画データを格納して蓄積する構成とすることによって達成される。

【0008】 また、請求項 2 に係る発明は、請求項 1 に記載のネットワークスキャナにおいて、前記フォルダをネットワークスキャナと配信先端末装置のいずれか、またはその両者に設定することを特徴としている。

【0009】 また、請求項 3 に係る発明は、請求項 1 または請求項 2 に記載のネットワークスキャナにおいて、前記属性は、ユーザ毎に各画データに対する処理可能な項目が設定されることを特徴としている。

【0010】 上記請求項 1 に係る発明の特徴によれば、フォルダに蓄積されて配信先端末装置に配信される画データにセキュリティの属性を付与している。このため、画データ毎のセキュリティを確保することができる。

【0011】 また、請求項 2 に係る発明においては、セキュリティの属性が付与された画データを格納して蓄積するフォルダを、ネットワークスキャナと配信先端末装置のいずれかに設定している。このように、通信ネットワークに接続されているある通信端末装置にフォルダを設定すれば他の通信端末装置ではフォルダを設定する必要がなく、通信ネットワークに接続された通信端末装置間でフォルダを共有できる構成としており、メモリ資源を節約できる。

【0012】 また、ネットワークスキャナと配信先端末装置の両者にフォルダを設定する場合には、例えばネットワークスキャナを他のネットワークに移動したような場合や、ネットワークスキャナのフォルダが破損した場合でも、データの復元が容易に行なえる。

【0013】 さらに、請求項 3 に係る発明においては、セキュリティの属性は、ユーザ毎に各画データに対する処理可能な項目が設定される。このため、各画データ毎に、特定のユーザはどのような処理を行なえるかが明瞭になり、画データを配信する際のセキュリティを高めることができる。

## 【0014】

【発明の実施の形態】 以下、本発明に係るネットワークスキャナの実施の形態について図により説明する。図 3

10

20

30

40

50

は、本発明のネットワークスキャナが使用される通信ネットワークの一形態を示す概略のブロック図である。図 3 において、LAN 5 には、ネットワークスキャナとして作用する FAX サーバ 1、画データの配信先端末装置であるファイルサーバ 2、クライアント PC 3、プリンタ 4 が接続されている。

【0015】FAX サーバ 1 で読み取り画像の画データを形成し、LAN 5 に接続されている配信先端末装置に前記画データを配信するものとする。ファイルサーバ 2 が配信先であれば、FAX サーバ 1 から出力された画データは、LAN 5 を介して D a の経路でファイルサーバ 2 に設定されたフォルダに入力される。

【0016】また、クライアント PC 3、プリンタ 4 が配信先の場合にも、LAN 5 を介してそれぞれの通信端末装置に設定されたフォルダに画データが入力される。なお、前記ファイルサーバ 2 に設定されたフォルダを、LAN 5 に接続された各通信端末装置で共有する構成とすることもできる。この場合には、ネットワークスキャナからファイル名が付与されて配信された画データは、順次ファイルサーバ 2 に設定されたフォルダに格納されて蓄積される。

【0017】このように、ファイルサーバ 2 に設定されたフォルダを通信ネットワーク上で共有する構成とする場合の各通信端末装置の処理について説明する。クライアント PC 3 は、LAN 5 を介して D b の経路でファイルサーバ 2 の前記フォルダにアクセスして画データの閲覧等の処理を行なう。同様にプリンタ 4 は、LAN 5 を介して D c の経路でファイルサーバ 2 の前記フォルダにアクセスして画データの印刷等の処理を行なう。

【0018】本発明においては、LAN 等の通信ネットワークに接続された通信端末装置のユーザが、ネットワークスキャナで形成された画データが格納されているフォルダにアクセスする際に、ユーザ毎に当該画データに対するセキュリティの属性を設定して、配信される画データに対するセキュリティが確保できる構成としている。

【0019】図 2 は、フォルダに格納されるデータ構成の例を示す説明図である。図 2 において、(b) の部分は、ネットワークスキャナで原稿を読み取り形成された画データである。(a) の部分は、画データ (b) に付与されるセキュリティの属性 (画データに対する処理をどのレベルまで実施できるか、すなわちユーザに許容される処理権限の項目を示す) であり、各画データ毎に設定される。

【0020】図 1 は、前記属性の例を示す説明図である。図 1 に示すように、セキュリティの属性は、ユーザ名と、処理可能な項目とをテーブルで対応させるものである。処理可能な項目として、当該画データについての「閲覧」、「編集」、「消去」、「印刷」を例示している。

【0021】前記各項目の中で、ユーザに処理権限がある項目には○印を付しており、処理権限がない項目には×印を付している。例えば、ユーザ名「yamamoto」は、当該画データの閲覧、編集の処理は可能であるが、消去、印刷の処理はできない。また、ユーザ名「sato h」は、当該画データの閲覧の処理は可能であるが、編集、消去、印刷の処理はできない。

【0022】図 1 に示したセキュリティの属性のテーブルでは、ユーザ名をアルファベットで表記しているが、各ユーザの識別子 (ID) で表記することもできる。なお、当該画データが複数頁で形成されている場合には、各頁毎に「閲覧」、「編集」、「消去」、「印刷」の処理ができるユーザを個別に設定しても良い。

【0023】図 1 に示したセキュリティの属性は、ユーザ固有の処理権限の項目として予め設定しておくことができる。例えば、前記「sato h」はすべての画データに対して閲覧の処理のみが可能であり、他の項目の処理は不可であるものと設定する。また、各画データ毎に、ユーザに許容される処理権限の項目を変えることができる。

【0024】例えば、前記ユーザ「sato h」は、ある画データの閲覧の処理は可能であるが、他の画データの閲覧の処理は不可と設定する。図 1 に示したようなセキュリティの属性は、ネットワークスキャナに設置された入力キーやマウス等の操作部により設定する。このようなセキュリティの属性を付与した共有フォルダは、FAX サーバ 1 に設定する他、前記のように通信ネットワークに接続された他の通信端末装置、例えば、ファイルサーバに設定することができる。

【0025】FAX サーバ 1 に共有フォルダを設定すると、通信ネットワークに接続された他の通信端末装置は前記 FAX サーバ 1 に設定された共有フォルダを利用できるので、メモリ資源を節約できる。また、前記他の通信端末装置に共有フォルダを設定すると、FAX サーバ 1 のメモリ資源を節約できる。

【0026】更に、FAX サーバ 1 に設定された共有フォルダをコピーして、他の通信端末装置に同じ共有フォルダを設定することもできる。この場合には、例えば FAX サーバ 1 を他のネットワークに移動したような場合や、FAX サーバ 1 の共有フォルダが破損した場合でも、データの復元が容易に行なえる。

【0027】図 4 は、本発明に適用される FAX サーバに設ける制御装置 20 の一例を示す概略のブロック図である。図 4 において、21 は各種信号やデータを処理するための超小型演算処理装置 (以下、MPU と略記する)、22 は FAX サーバの各種動作に必要なデータやプログラム格納される ROM、23 は管理データ等が格納される RAM である。

【0028】24 は画データを記録紙に出力するプリンタ、25 は原稿を読み取り、白黒 2 値のイメージデータ

である画データを出力する読取部、26はキーボードやマウス等からなる操作部である。FAXサーバは、ネットワークインターフェイス(I/F)27を介してLAN5に接続される。FAXサーバは、サービス総合デジタル網(ISDN)のインターフェイス(I/F)28、デジタル回線終端装置(DSU)29を介してISDNに接続される。また、回線制御部(NCU)30を介して公衆回線網(PSTN)に接続される。

【0029】31はPSTNを介して相手先のファクシミリ装置との間で送受信されるファクシミリデータを変調、復調するモデムであり、モデム31とNCU30とはアナログ信号線31aで接続される。

【0030】符号・復号部32は、画データを符号化し、また画データを復号化する。図形文字発生部33は、文字コードデータをイメージデータに変換する。34は陰極線管(CRT)や液晶表示器(LCD)を用いた表示部、35は画データに日時を記入するために用いる時計部、36は通信管理記録と画データを記憶するハードディスク(HD)、37は内部バスである。なお、記憶容量をそれほど必要としない場合には、ハードディスク(HD)に代えて画像メモリを用いる。

【0031】図5は、本発明のネットワークスキャナの処理手順を示すフローチャートである。次にこのフローチャートについて説明する。

【0032】(1)ステップS1で、ネットワークスキャナの処理プログラムを開始し、ステップS2の処理で、読み取り原稿をセットする。次に、ステップS3の処理に移行して、画データを格納する共有フォルダの宛先と、セキュリティの属性を指定する。

【0033】(2)次に、ステップS4の処理で原稿を読み取り、画データの符号化処理を行なう。続いて、ステップS5の処理で、属性および画データを画像メモリに格納し、ステップS6で処理プログラムを終了する。

【0034】図6は、画データにアクセスするクライアントPCの処理手順を示すフローチャートである。次にこのフローチャートについて説明する。

【0035】(1)ステップS11でクライアントPCの処理プログラムを開始し、ステップS12の処理で、アクセスするファイル指定を行なう。次に、ステップS13の処理で、セキュリティ属性をチェックする。続いてステップS14の処理で、画データが格納されたフォルダのファイルに対して、ユーザがアクセスする権限を有しているかどうかを判定する。この判定結果がNOであれば、ステップS16で処理プログラムを終了する。

【0036】(2)ステップS14の判定結果がYESであれば、ユーザはファイルにアクセスする権限を有していることになるので、ステップS15の処理に移行する。ステップS15の処理では、当該ファイル名の画データについて、閲覧、編集、消去、印刷等の処理の中で許可されている処理を行なう。次にステップS16で処

理プログラムを終了する。

【0037】図3において、LAN5に他のFAXサーバを接続し、FAXサーバ1から他のFAXサーバに画データを配信することもできる。この場合には、当該他のFAXサーバは、FAXサーバ1の配信先端末装置として作用する。

【0038】また、当該他のFAXサーバが、ファイルサーバ2に設定された共有フォルダから画データを読み出して、他の通信端末装置に配信することができる。更に、当該他のFAXサーバで原稿を読み取り形成された画データにセキュリティの属性を付与して、共有フォルダとして設定された自機内のフォルダに格納することができる。

【0039】

【発明の効果】以上詳述したように請求項1に係る発明によれば、フォルダに蓄積されて配信先端末装置に配信される画データにセキュリティの属性を付与している。このため、画データ毎のセキュリティを確保することができる。

【0040】また、請求項2に係る発明においては、セキュリティの属性が付与された画データを格納して蓄積するフォルダを、ネットワークスキャナと配信先端末装置のいずれかに設定している。このように、通信ネットワークに接続されているある通信端末装置にフォルダを設定すれば他の通信端末装置ではフォルダを設定する必要がなく、通信ネットワークに接続された通信端末装置間でフォルダを共有できる構成としており、メモリ資源を節約できる。

【0041】また、ネットワークスキャナと配信先端末装置の両者にフォルダを設定する場合には、例えばネットワークスキャナを他のネットワークに移動したような場合や、ネットワークスキャナのフォルダが破損した場合でも、データの復元が容易に行なえる。

【0042】さらに、請求項3に係る発明においては、セキュリティの属性は、ユーザ毎に各画データに対する処理可能な項目が設定される。このため、各画データ毎に、特定のユーザはどのような処理を行なえるかが明瞭になり、画データを配信する際のセキュリティを高めることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係るネットワークスキャナで設定する画データのセキュリティの属性を示す説明図である。

【図2】セキュリティの属性が付与された画データを示す説明図である。

【図3】ネットワークスキャナがLANに接続された例を示すブロック図である。

【図4】FAXサーバの制御装置を示すブロック図である。

【図5】本発明の処理手順を示すフローチャートであ

る。

【図 6】本発明の処理手順を示すフローチャートである。

【符号の説明】

1 FAXサーバ (ネットワークスキャナ)

2 ファイルサーバ

3 プリンタ

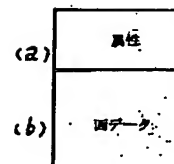
4 クライアントパーソナルコンピュータ (PC)

5 ユーザ構内通信網 (LAN)

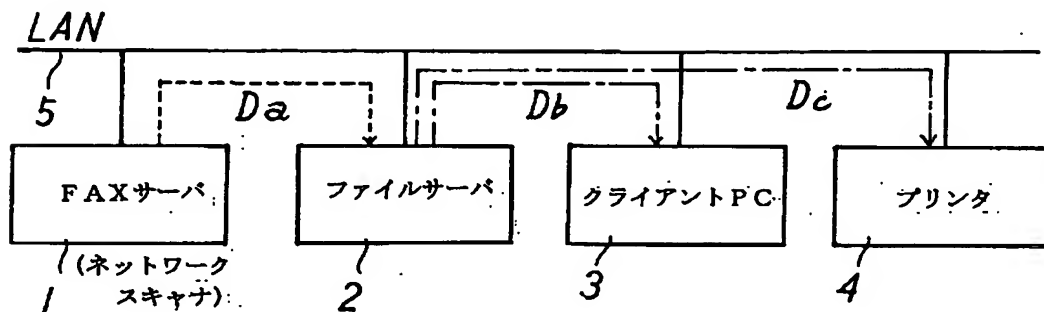
【図 1】

ユーザ \ 項目	閲覧	編集	削除	印刷
tanaka	○	○	×	×
tanaka	○	○	○	○
tanaka	○	×	×	×
tanaka	○	×	○	×

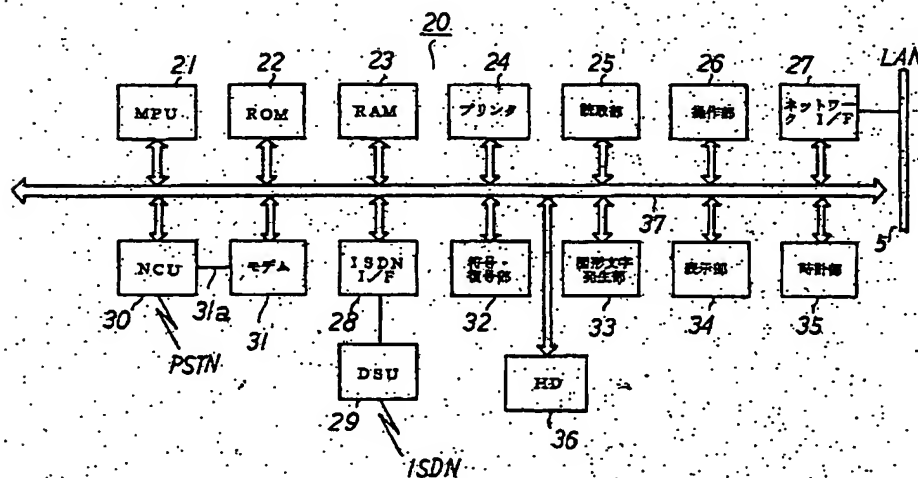
【図 2】



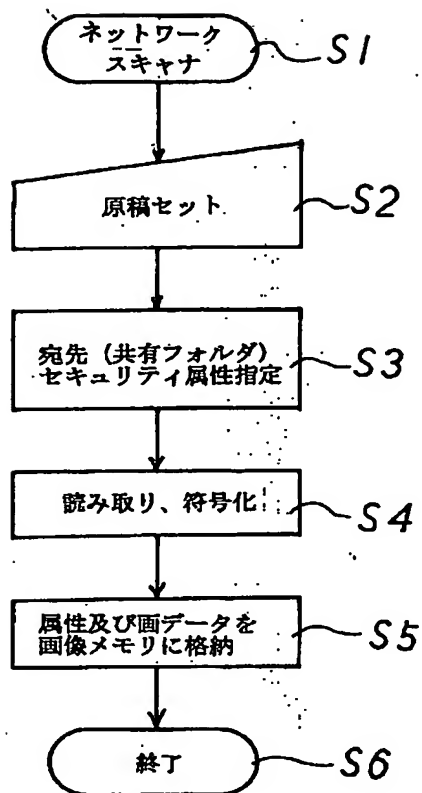
【図 3】



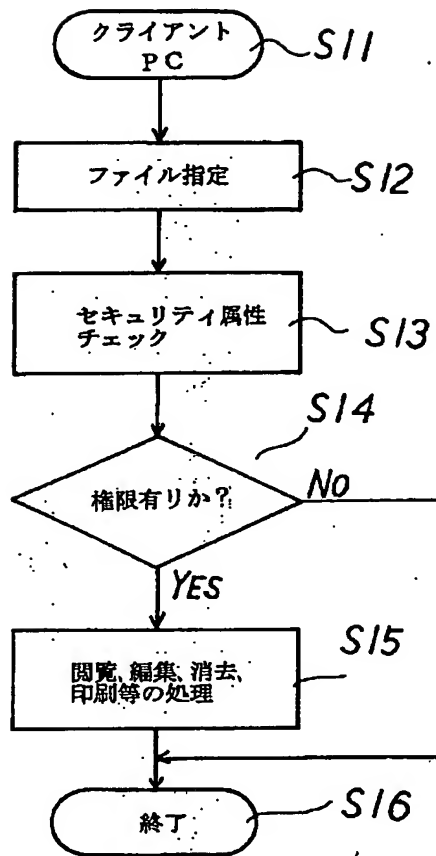
【図 4】



【図5】



【図6】



## 【手続補正書】

【提出日】平成12年8月31日(2000. 8. 3

【図5】

1)

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0033

【補正方法】変更

【補正内容】

【0033】(2)次に、ステップS4の処理で原稿を読み取り、画データの符号化処理を行なう。続いて、ステップS5の処理で、属性および画データを共有フォルダに格納し、ステップS6で処理プログラムを終了する。

## 【手続補正2】

【補正対象書類名】図面

【補正対象項目名】図5

【補正方法】変更

【補正内容】

